UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/487,726	01/19/2000	Toru Sumino	Q57604	3499

7590 05/26/2004

Sughrue Mion ZInn Macpeak & Seas PLLC
2100 Pennsylvania Avenue N W
Washington, DC 20037-3213

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 05/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/487,726	SUMINO, TORU	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *18 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,5 and 7-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,5,7-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This Office action is in response to the amendment, Paper No. 10, filed on March 18, 2004. The original application contained claims 1 – 10. Per the received amendment, claims 2, 4, and 6 have been cancelled and claims 1, 9, and 10 have been amended. Presently pending claims are 1,3, 5, and 7-10.

Response to Arguments

2. Applicant's arguments filed on March 18, 2004, Paper No. 10, have been fully considered but they are not persuasive because of the following reasons:

Regarding currently amended claim 1, the applicant argues that the cited prior art does not disclose "an individual authentication system" that comprises "an individual authentication card" that "has a function of collating the stored identification number with the identification number transmitted by the identification number input device." These arguments are not found persuasive in view of new prior art Teicher et al. (U.S. Patent 6,257,486). Teicher teaches a smart card system in which a personal identification number (PIN) is authenticated directly by the smart card itself, and not propagated outside of the smart card (column 14 lines 15 – 39). The authentication is done by an authentication unit (Figure 11 item 1110), which, according to Teicher, can be

incorporated into the smart card processor. Teicher states that authenticating the PIN directly on the smart card itself makes it impossible for another device in the system to covertly obtain the PIN. The new prior art can be logically combined with the previous prior art rejection of Moussa et al. (U.S. Patent 6,035,406) and Dunn et al. (U.S. Patent 5,987,155) to achieve an individual authentication system which can authenticate a user by means of biological input, a password, and by an identification number which is collated directly on the smart card. Accordingly, the rejection for the pending claims 1,3,5, and 7-10 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim 1,3, and 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moussa et al. (U.S. 6,035,406) in view of Dunn et al (U.S. 5,987,155) further in view of Teicher et al. (U.S. Patent 6,257,486).

Regarding claim 1, Moussa discloses an individual authenticating system for authenticating the user of a data processing device storing a password (Fig.1) comprising:

an individual authentication card for storing biological information and a password for identifying a registered user (column 3, lines 34-37);

a card reader for reading out the biological information and the password stored in the card (item 130 of Figure 1, column 3 lines 8 – 13);

means for respectively collating the biological information and the password read from the card reader with the biological information read from the biological information input device and the password stored in the data processing device (column 4 lines 1-12, column 4 lines 56-64);

wherein the data processing device has an identification number input device by which the user inputs an identification number (column 4 lines 1-7, items 221 –224 of Figure 2).

Moussa does not explicitly describe:

a biological input device for inputting the biological information from a user; and

the card stores an identification number for identifying the registered user, and has a function of collating the stored identification number with the identification number transmitted by the identification number transmitted by the identification number input device.

Dunn teaches a biological information input device for inputting biological information from a user (Figure 2, column 4 lines 30-47);

Moussa teaches a login service (column 3 lines 24-28) that maintains an authentication database that stores fingerprint information. Biometric input and authentication devices were well-known in the art at the time the invention was made, and its implementation,

such as delineated by Dunn, in conjunction with the teachings of Moussa would have been obvious to one of ordinary skill in the art at the time the invention was made because if the authentication database taught by Moussa was to be removed, a biometric input device would be needed for the biometric authentication of users. The addition of such a biometric input device would add the flexibility to authenticate users on-site rather than relying on a remote database and provides for another user input required to access a system adding another security measure.

Teicher teaches a card storing an identification number for identifying the registered user with a function of collating the stored information with the identification number transmitted by the identification number input device (column 14 lines 15 – 39). Teicher teaches a smart card system in which a personal identification number (PIN) is authenticated directly by the smart card itself, and not propagated outside of the smart card. The authentication is done by an authentication unit (Figure 11 item 1110), which, according to Teicher, can be incorporated into the smart card processor. Teicher states that authenticating the PIN directly on the smart card itself makes it impossible for another device in the system to covertly obtain the PIN. Therefore it would have been obvious to one of ordinary skill in the art to combine the teachings of Moussa with Dunn and Teicher to add flexibility to authenticate users on-site, to provide another user input required to access a system, increasing security, and by collating the PIN directly on the smart card, making it impossible to for another device in the system to covertly obtain the PIN.

Claim 3 is rejected as applied above in rejecting claims 1. Furthermore, Moussa discloses an individual authentication system, wherein the biological information is fingerprint data (column 3 line 37).

Regarding claim 7, Moussa teaches an authentication system, wherein the card is an IC card storing at least the biological information and the password for identifying registered users. Moussa does not explicitly describe that this information is stored as electrical signals. Moussa mentions that the physical token includes a stored password and biometric information (column 3 lines 34-37). It was known in that art at the time of invention that IC cards use electric signals to store information. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to store the password and biometric as electrical signals on the IC card since information is converted to electric signals before it is passed to an IC card.

Claims 8 and 9 are rejected applied as above in rejecting claim 1. Furthermore, Moussa discloses an individual authentication system wherein one or both of the biological information and the password are encrypted using an encryption algorithm (column 3 lines 29-37).

Regarding claim 10, Moussa teaches an authentication system containing a card reader (item 130 of Figure 1, column 3 lines 8-13), and an identification number input device (item 120 of Figure 1). Moussa does not explicitly describe a biological input device,

teaching a login service (column 3 lines 24-28) that maintains an authentication database that stores fingerprint information that is collated from the biological information stored on the IC card. Dunn teaches a biological input device where a user can be authenticating by providing biometric input to a biometric input device. The addition of such a biometric input device would add the flexibility to authenticate users on-site rather than relying on a remote database and provides for another user input required to access a system adding another security measure. Combining these three elements into a single device should have been obvious to one of ordinary skill in the art at the time the applicant's invention was made because the benefit of authenticating a user using both an IC card and biometric authentication provides a plurality of security factors to make a security system more robust and flexible without the use of an authentication database.

4. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Moussa et al. (U.S. 6,035,406) in view of Dunn et al (U.S. 5,987,155) further in view of Teicher et al. (U.S. Patent 6,257,486) in further view of Pearson et al. (U.S. 5,991,408).

Claim 5 is rejected as applied above in rejecting claims 3, respectively. Furthermore, Moussa discloses an individual authentication system, wherein the biological information is fingerprint data, where this data is stored on an IC card. Moussa does not explicitly describe a "plurality of fingerprint data."

Pearson teaches:

an individual authentication system wherein the biological information is a plurality of fingerprint data (column 4 lines 63-67).

Pearson teaches that a plurality of fingerprint data can be used to overcome variations in the biometric element. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to include a plurality of fingerprint data as delineated by Pearson in conjunction with the system of Moussa, Dunn, and Teicher to get this benefit of overcoming variations in a biometric element in situations where the biometric element may have been slightly changed. The implementation of a plurality of fingerprint data with the teachings of Moussa in conjunction with Dunn and Teicher would provide the benefit of being able to authenticate users based on more than one set of biometric data, creating a more robust and redundant biometric authentication system.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 703-305-8892. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

KA
05/18/04

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100